TRABAJO DE FIN DE GRADO

GRADO EN DERECHO

CURSO ACADÉMICO 2020-2021

Protección de datos y herramientas tecnológicas para la prevención del Covid-19: análisis a la luz de dos modelos contrapuestos (España vs Emiratos Árabes Unidos)

Data protection and technological tools for the prevention of Covid-19: an analysis in light of two contrasting models (Spain vs United Arab Emirates)

AUTOR:

María Pilar Mendoza García

DIRECTOR:

Prof. Dr. Joaquín Cayón de las Cuevas

Marzo, 2021

RESUMEN:

El presente trabajo analiza la tensión entre protección de datos y salud pública, utilizando dos *case studies* que ponen de relieve dos modelos antagónicos: el de España, tributario de la disciplina de la Unión Europea en la materia, y el de los Emiratos Árabes Unidos, países de hondas diferencias culturales, políticas y de tradición jurídica. Particularmente, se examina el régimen jurídico de la utilización de herramientas tecnológicas para la prevención del Covid-19, con especial atención en las apps de rastreo y geolocalización. En el caso español, si bien existe una prohibición general de tratamiento de datos de salud, existen varios títulos de legitimación que permiten ciertos tratamientos por razones de salud pública, si bien sujetos a determinadas garantías y precauciones advertidas tanto por la agencia española de protección de datos como por el Comité Europeo de Protección de Datos. En el caso emiratí, nos encontramos ante un modelo menos sensible al respeto al derecho fundamental a la protección de datos, que en muchos casos supuestos establece la obligatoriedad del uso de determinadas herramientas o las condiciona para el acceso a determinados servicios. La finalidad última del trabajo radica en contrastar un sistema garantista frente a un sistema laxo en la materia.

ABSTRACT:

This paper analyzes the tension between data protection and public health, using two case studies that highlight two antagonistic models from countries with deep cultural, political and legal differences: the Spanish one, which is based on the the European Union legal framework in this this field, and the system from the United Arab Emirates. In particular, the legal regime of the use of technological instruments for the prevention of Covid-19 is examined, with special attention to tracing and geolocation apps. In the Spanish case, even though there is a general prohibition on the processing of health data, there are several legitimization titles that allow certain processing for public health reasons, albeit subject to certain guarantees and precautions, as noted by both the Spanish Data Protection Agency and the European Data Protection Committee. In the case of the United Arab Emirates, we are faced with a model that is less sensitive to respect for the fundamental right to data protection. In fact, in many cases it lays down a compulsary use of certain tools or sets up conditions for accessing certain services. The ultimate aim of this paper is to contrast a system that guarantees the right to data protection with a lax system in this field.

INDICE

1. INTRODUCCIÓN

Como es sobradamente conocido, el Covid-19 es una enfermedad infecciosa causada por un tipo de coronavirus descubierto recientemente, el SARS-CoV-2. Esta nueva enfermedad fue identificada por primera vez en Wuhan, China, a finales de 2019. La rápida evolución, virulencia, mortandad y expansión de la enfermedad ha provocado que la epidemia adquiriese el *status* de pandemia. Así, el 11 de marzo de 2020, el Director General de la Organización Mundial de la Salud, Dr. Tedros Adhanom Ghebreyesus, declaró que la crisis provocada por el coronavirus denominado Covid-19 tenía carácter de pandemia[1].

Ante la emergencia sanitaria, se han venido planteando diferentes medidas de contención y respuesta[2] que afectan a la protección de datos de carácter personal. Por consiguiente, procede analizar el grado de limitación del derecho fundamental a la protección de datos por razones de salud pública, en particular, en relación con los datos relativos a la salud y los datos de geolocalización de los eventuales afectados.

En este sentido, el objetivo fundamental que persigue este trabajo radica en estudiar la tensión entre privacidad y salud pública, utilizando dos *case studies* que ponen de relieve dos modelos antagónicos: el de España y el de los Emiratos Árabes Unidos, países de hondas diferencias culturales, políticas y de tradición jurídica. En este sentido, cabe avanzar la necesidad de conciliar las necesidades de lucha frente a la pandemia –que requiere la utilización de soluciones tecnológicas- con la protección de datos de datos personales, ponderando este complejo binomio de una manera que permita una gestión de la pandemia que sea eficaz pero también respetuosa con los derechos fundamentales.

[1] La literatura producida sobre el Covid-19 es interminable. No obstante, para una visión global de su impacto puede consultarse HISCOTT, J., ALEXANDRIDI, M., MUSCOLINI, M., TASSONE. E., PALERMO, E., SOULTSIOTI, M., ZEVINI, A. (2020): "The global impact of the coronavirus pandemic", *Cytokine Growth Factor Rev*, nº 53, pp. 1-9. KHAN, M., ADIL, S.F., ALKHATHLAN, H.Z., TAHIR, M.N., SAIF, S., KHAN, M., KHAN, S.T. (2021): "COVID-19: A Global Challenge with Old History, Epidemiology and Progress So Far". *Molecules*, nº 26(1), pp. 1-25. NICOLA, M., ALSAFI, Z., SOHRABI, C., KERWAN, A., AL-JABIR, A., IOSIFIDIS, C., AGHA, M., AGHA, R. (2020): "The socio-economic implications of the coronavirus pandemic (COVID-19): A review". *International Journal of Surgery*, nº 78, pp.185-193.

[2] Un resumen en el caso español puede encontrarse en CAYÓN DE LAS CUEVAS, J., OCHAGAVÍAS COLAS J.I. (2020): "Overview of the COVID-19 legal framework in Spain: from the state of alarm to the new normal" *EAHL Newsletter*, nº 3, pp. 73-76.

2. EL MODELO GARANTISTA DE PROTECCIÓN DE DATOS EN ESPAÑA

2.1. NORMATIVA EUROPEA

2.1.1. Fundamento del Reglamento General de Protección de Datos

Hablar del régimen jurídico de protección de datos en España requiere lógicamente comenzar analizando la normativa comunitaria en la materia, cuya piedra angular es el Reglamento General de Protección de Datos (en adelante RGPD)[3], norma que instaura un conjunto de normas directamente aplicables en todos los Estados miembros. El RGPD, que deroga la anterior Directiva de Protección de Datos de 1985[4], culmina un largo proceso iniciado en 2012, cuando la Comisión Europea presentó el *Data Protection Package*, alumbrando un nuevo marco normativo de garantía del derecho a la protección de datos[5].

Debemos hacer varias consideraciones importantes en relación a este Reglamento. En primer lugar, el considerando 1 del RGPD pone de relieve la positivización de este derecho, que aparece recogido en el artículo 8.1 de la Carta de los Derechos Fundamentales de la Unión Europea y en el artículo 16.1 del Tratado de Funcionamiento de la Unión Europea. En segundo lugar, en atención a la libre circulación de los datos personales, debemos atender al artículo 1.3 RGPD. Podemos observar en el mismo el contrapunto de la protección de datos, la circulación vs la protección de los mismos, el legislador realiza una tarea de armonización. Es decir, la protección con el consiguiente tratamiento no obsta garantizar su libre circulación. Esta idea la refuerza el considerando 4 del RGPD, al poner de relieve la esencia misma de los datos personales, que no es otra que es servir a la humanidad, avalando la función que tienen en la sociedad. Así, se configura como un derecho no absoluto que debe ejercitarse con arreglo al principio de proporcionalidad. Por último, debemos traer a colación el considerando 8, pues abre la veda a los Estados Miembros, a que realicen una labor de desarrollo de las normas del RGPD para que, a través del derecho doméstico, puedan establecer especificaciones o

[3] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016.
[4] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos
[5] RALLO LOMBARTE, A. (2019). "El nuevo derecho de protección de datos". *Revista Española de Derecho Constitucional,* 116, pp. 47-48.

restricciones, en la medida en que sea necesario por razones de coherencia y para que las disposiciones nacionales sean comprensibles para sus destinatarios.

Sentadas estas premisas de partida, encontramos el objeto del RGPD en su artículo 1.1 que señala que *"(…) establece las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos (…)"*. Profundizando en el contenido del precepto, podemos observar que el derecho a la protección de datos goza del tratamiento de derecho fundamental. Como destaca RALLO LOMBARTE, "lo más relevante reside en que el fundamento constitucional del derecho fundamental de protección de datos se ha desplazado del ámbito nacional al europeo y, sobre este último anclaje, se ha normativizado un derecho fundamental homogéneo en toda la Unión Europea"[6]. Por consiguiente, el RGPD pone claramente de manifiesto su intención de instaurar una adecuada red tuitiva de este derecho fundamental.

2.2. Ámbito de aplicación

Respecto al ámbito de aplicación del RGPD, deben considerarse sus artículos 2 y 3, así como los considerandos explicativos que figuran en su exposición de motivos. Comenzando por el ámbito de aplicación personal, éste alude a las personas físicas independientemente de su nacionalidad o de su lugar de residencia, en relación con el tratamiento de sus datos personales. A su vez, el considerando 27 que establece otra exclusión con respecto a los datos de las personas fallecidas. Por ello, el RGPD tampoco será aplicable a la protección de los datos personales de personas fallecidas, siendo los Estados miembros los que resultan competentes para establecer la normativa reguladora del tratamiento de los datos de aquellas. Finalmente, el RGPD no disciplina el tratamiento de datos personales relativos a personas jurídicas (considerando 14).

En cuanto al ámbito de aplicación material, el artículo 2.2 RGPD excluye tratamiento de datos personales: a) en el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión; b) por parte de los Estados miembros cuando lleven a cabo actividades comprendidas en el ámbito de aplicación del capítulo 2 del título V del TUE; c) efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas; d) por parte de las autoridades competentes con

[6] RALLO LOMBARTE, A. (2019), *ob. cit.*, p. 49.

fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención.

En relación con el ámbito material, debemos realizar una doble disección respecto de los datos que gozan de la condición de tratamiento sujeto al RGPD y cuáles no. Por ello, acudimos el artículo 2.1 REPD que establece que éste será de aplicación tanto "*al tratamiento total o parcialmente automatizado de datos personales, como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero"*. Por tanto, la protección del reglamento abarca tanto el tratamiento automatizado de datos personales, como su tratamiento no automatizado, es decir, un tratamiento manual de los mismos, contenidos o destinados a ser incluidos en un fichero.

Sin embargo, el considerando 15, matiza *"(…) los ficheros o conjuntos de ficheros, así como sus portadas, que no estén estructurados con arreglo a criterios específicos, no deben entrar en el ámbito de aplicación del presente Reglamento"*. De esta manera, atendiendo a la otra cara de la disección del artículo 2 REPD, el depósito de datos de forma no estructurada, sin observar un criterio de ordenación que pudiera permitir la búsqueda e identificación de los datos de una persona, no resultaría sometido al régimen protector del RGPD.

Por otra parte, el RGPD no resulta aplicable al tratamiento de datos personales, en los siguientes casos (artículo 2.2 RGPD):

> "*a) en el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión;*
> *b) por parte de los Estados miembros cuando lleven a cabo actividades comprendidas en el ámbito de aplicación del capítulo 2 del título V del TUE;*
> *c) efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas;*
> *d) por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención".*

Los apartados a) y b) vienen a establecer dos exclusiones. No estarían sometidas a las disposiciones del RGPD, en primer lugar, a las actividades relativas a la seguridad nacional en tanto que resultan ser actividades excluidas del ámbito del Derecho de la Unión. En segundo lugar, esta norma tampoco se aplicaría al tratamiento de datos de carácter personal por los Estados miembros en el ejercicio de las actividades relacionadas con la política exterior y de seguridad común de la Unión.

El apartado c) establece la denominada *excepción doméstica.* En este sentido, el considerando 18, aclara que "*entre las actividades personales o domésticas cabe incluir la correspondencia y la llevanza de un repertorio de direcciones, o la actividad en las redes sociales y la actividad en línea realizada en el contexto de las citadas actividades".* Pero, en las últimas líneas del considerando se establece un contrapunto a la exclusión, al indicar que *"no obstante, el presente Reglamento se aplica a los responsables o encargados del tratamiento que proporcionen los medios para tratar datos personales relacionados con tales actividades personales o domésticas."*

Por último, el apartado d) realiza la última exclusión, excluyento los tratamientos *con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales*. La razón de ser de esta exclusión es que el legislador, prevé una concreta regulación con respecto a las actividades de tratamiento de tales fines en la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo[7].

Finalmente, en lo que respecta al ámbito de aplicación territorial, el RGPD se aplica en el ámbito territorial de la Unión Europea, pero el legislador le atribuye un efecto *extra muros* de los lindes comunitarios. En este sentido, el artículo 3 señala que el Reglamento se aplica:

> "*-al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no.*

[7] Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

- al tratamiento de datos personales de interesados que residan en la Unión por parte de un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con:

a) la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago, o

b) el control de su comportamiento, en la medida en que este tenga lugar en la Unión."

Para un mejor entendimiento del precepto debemos realizar una serie de matizaciones. El legislador aclara en el considerando 22 lo que se debe entender por el concepto de "establecimiento" que *"implica el ejercicio de manera efectiva y real de una actividad a través de modalidades estables".* A este respecto, no es baladí *"la forma jurídica que revistan tales modalidades, ya sea una sucursal o una filial con personalidad jurídica (...)".*

A su vez, como ya hemos indicado, en los supuestos en el que el responsable o encargado no estén establecidos en la Unión, debe precisarse si aquel ofrece servicios o bienes a interesados en uno o varios de los Estados miembros de la Unión. Por consiguiente, hay que tener en cuenta el considerando 24 y, en definitiva, tener claro que el hecho de que el responsable del tratamiento de datos esté en un país tercero no debe impedir la protección de las personas considerada en el RGPD.

2.2. IMPLEMENTACIÓN EN LA LEGISLACIÓN DOMÉSTICA

El contenido del RGPD se completó en la normativa española a través de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (en adelante LOPDGDD). El objeto de la norma radica en adaptar la legislación española al RGPD (artículo 1.a), vigente ya desde el 25 de mayo de 2018, así como completar sus disposiciones.

Por consiguiente, la LOPDGDD pretende amparar la intimidad, privacidad e integridad del individuo, cuyo sustento constitucional descansa en el artículo 18.4 de la Constitución Española. No obstante, no se explicita el reconocimiento del derecho de protección de datos ni asegura un contenido constitucional mínimo del mismo[8]. Sin embargo,

[8] RALLO LOMBARTE, A. (2019), *ob. cit.*, pp. 56.

la doctrina constitucional se ha encargado de anclar en este precepto constitucional el reconocimiento de un derecho fundamental autónomo a la protección de datos personales, indicando que:

> *"Estamos ante un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la CE llama "la informática"*[9].

En cuanto a su ámbito de aplicación el artículo 2.2.a) LOPDGDD, tributario del RGPD, excluye los tratamientos a su vez excluidos del ámbito de aplicación del RGPD, sin perjuicio de lo dispuesto en los apartados 3[10] y 4[11] de este artículo. Tampoco se aplica a los tratamientos de datos de personas fallecidas, sin perjuicio de lo establecido en el artículo 3 (artículo 2.2.b), ni a los tratamientos sometidos a la normativa sobre protección de materias clasificadas (artículo 2.2.c)."

2.3. PROTECCIÓN DE DATOS EN EL CONTEXTO SANITARIO

Interesa específicamente qué son los datos relativos a la salud, cuya definición encontramos en el artículo 4.15 RGPD como:

> *"datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud."*

A su vez, debemos tener en cuenta el considerando 35 del Reglamento, que hace una tarea de especificación respecto a los datos relativos a la salud, exponiendo que entran bajo dicho concepto:

---

[9] STC 254/93, de 20 de julio. El contenido mínimo del derecho a la protección de datos puede verse en dos sentencias de la misma fecha: STC 290/2000, de 30 de noviembre, y STC 292/2000, de 30 de noviembre.

[10] Los tratamientos a los que no sea directamente aplicable el RGPD por afectar a actividades no comprendidas en el ámbito de aplicación del Derecho de la Unión Europea, se regirán por lo dispuesto en su legislación específica si la hubiere y supletoriamente por lo establecido en el citado reglamento y en la presente ley orgánica. Se encuentran en esta situación, entre otros, los tratamientos realizados al amparo de la legislación orgánica del régimen electoral general, los tratamientos realizados en el ámbito de instituciones penitenciarias y los tratamientos derivados del Registro Civil, los Registros de la Propiedad y Mercantiles

[11] El tratamiento de datos llevado a cabo con ocasión de la tramitación por los órganos judiciales de los procesos de los que sean competentes, así como el realizado dentro de la gestión de la Oficina Judicial, se regirán por lo dispuesto en el RGPD y la LOPDGDD, sin perjuicio de las disposiciones de la Ley Orgánica 6/1985, de 1 julio, del Poder Judicial, que le sean aplicables.

"(…) todo número, símbolo o dato asignado a una persona física que la identifique de manera unívoca a efectos sanitarios; la información obtenida de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal, incluida la procedente de datos genéticos y muestras biológicas, y cualquier información relativa, a título de ejemplo, a una enfermedad, una discapacidad, el riesgo de padecer enfermedades, el historial médico, el tratamiento clínico o el estado fisiológico o biomédico del interesado, independientemente de su fuente, por ejemplo un médico u otro profesional sanitario, un hospital, un dispositivo médico, o una prueba diagnóstica in vitro".

Sentado este concepto amplio de datos de salud, a raíz de la crisis sanitaria ocasionada por la Covid-19, asistimos a un proceso de investigación clínica acelerada que ha planteado dudas sobre la posibilidad de tratar datos personales de los ciudadanos[12]. Así, se han puesto de manifiesto luces y sombras de la regulación de la protección de datos. La realidad epidemiológica ha demostrado la necesidad de incrementar el procesamiento de datos en el ámbito de la salud. Analizando el derecho a la protección de datos desde el punto de vista de la crisis sanitaria de la Covid-19, la doctrina ha subrayado la necesidad de *"ponderar el potencial impacto en los derechos que garantizan la vida privada de las personas, y otros instrumentalmente relacionados, con los fines que persigue el derecho a la protección de la salud, incluida la salud pública (artículo 43 Constitución española). Debe señalarse que, en un contexto pandémico, el derecho a la protección de la salud, como principio rector de la política social y económica, cumple una función instrumental crucial en relación con la dignidad humana (artículo 10 CE) y los derechos a la vida del artículo 15 CE y a la seguridad (artículo 17 CE) en la medida, en este último caso, en el que la salud pública adquiere un valor esencial para la garantía del orden público y la convivencia democrática"*[13].

Todo derecho que implique en su ejercicio la posible colisión con otros bienes jurídicos, debe someterse a un juicio de proporcionalidad en su ejercicio. Por consiguiente, dicho juicio requiere traer a colación una serie de presupuestos que hay que tener en cuenta. En este sentido, MARTÍNEZ MARTÍNEZ pone de relieve dos premisas básicas: "*a) Los derechos fundamentales no se configuran como derechos ilimitados. b) La técnica de ponderación debe analizar la injerencia en el derecho a la vida privada desde un juicio*

[12]MARTÍNEZ MARTÍNEZ, R. (2020). "Los tratamientos de datos personales en la crisis del COVID-19. Un enfoque desde la salud pública". *Diario La Ley*, nº 9604.
[13] MARTÍNEZ MARTÍNEZ, R. (2020), *ob. cit.*

basado en la idoneidad y la necesidad de la medida, regido por el principio de mínima intervención"[14].

Como ya se expuso en el principio del presente trabajo, el RGPD constituye la piedra angular en materia de protección de datos, por lo que es necesario traer a colación el principio de primacía del Derecho comunitario, por lo que no hay que olvidar que el RGPD es de alcance general a todos los estados miembros. En este sentido, se ha propuesto considerar al RGPD como fuente de Derecho a la hora de identificar excepciones a las facultades que integran el contenido esencial de este derecho fundamental[15].

Por tanto, el derecho a la protección de datos se simplifica a un poder de disposición y ese poder de disposición implica la facultad conferida a la persona para decidir: i) si esos datos los facilita o no a un tercero (Estado o un particular); ii) qué datos puede obtener dicho tercero y la información al individuo acerca de quién posee esos datos personales; y, iii) con qué fin, de manera que puede oponerse tanto a su uso como a su posesión. Hay una triple consideración, por tanto, del poder de disposición

Es sabido que toda facultad tiene un haz y un envés. El haz hace referencia a que ese poder de disposición implica necesariamente consentimiento por parte de la persona, es decir, consentimiento al conocimiento y al tratamiento. El envés implica la posibilidad del tratamiento de datos personales sin consentimiento, es decir, una excepción legal al contenido esencial del derecho fundamental. Centrándonos, en la situación pandémica, el artículo 9.2 i) RGPD permite:

> *"el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional"*[16].

En base a la regulación actual, el tratamiento de datos referentes a la salud forma parte de lo que se denominan las "categorías especiales de datos personales", que el

[14] MARTÍNEZ MARTÍNEZ, R. (2020), *ob. cit.*
[15] MARTÍNEZ MARTÍNEZ, R. (2020), *ob. cit.*
[16] AEPD (2020): Informe AEPD N/REF: 0017/2020, de 12 de marzo, avala todos aquellos tratamientos necesarios para alcanzar los objetivos de salud pública.

considerando 51 del RGPD califica como aquéllos *"por su naturaleza, son particularmente sensibles en relación con los derechos y las libertades fundamentales"*. Adicionalmente, para aclarar la regulación relativa a los datos de salud, debemos traer a colación el considerando 46 del RGPD que afirma que:

> *"El tratamiento de datos personales también debe considerarse lícito cuando sea necesario para proteger un interés esencial para la vida del interesado o la de otra persona física. En principio, los datos personales únicamente deben tratarse sobre la base del interés vital de otra persona física cuando el tratamiento no pueda basarse manifiestamente en una base jurídica diferente. Ciertos tipos de tratamiento pueden responder tanto a motivos importantes de interés público como a los intereses vitales del interesado, como por ejemplo cuando el tratamiento es necesario para fines humanitarios, incluido el control de epidemias y su propagación, o en situaciones de emergencia humanitaria, sobre todo en caso de catástrofes naturales o de origen humano."*

Por consiguiente, vemos cómo el propio RGPD reconoce que la base legal en el tratamiento de datos puede ser plural. Para DOMÍNGUEZ ÁLVAREZ, el RGPD reconoce explícitamente dos bases jurídicas legitimadoras del tratamiento de datos personales diferenciadas: el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física (art. 6.1.d); y el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento (art. 6.1.e)[17].

Centrándonos en el artículo 6.1 d) RGPD, el autor aclara que el interés vital no sólo se refiere al interés vital del interesa dino que engloba también *"los intereses vitales de otra persona."*. Por ello, "dicha base jurídica del tratamiento —el interés vital— puede ser suficiente para los tratamientos de datos personales dirigidos a proteger a todas aquellas personas susceptibles de ser contagiadas en la propagación de una epidemia, lo que justificaría, desde el punto de vista de tratamiento de datos personales, en la manera más amplia posible, las medidas adoptadas a dicho fin, incluso aunque se dirijan a proteger personas innominadas o en principio no identificadas o identificables, por cuanto los intereses vitales de dichas personas físicas habrán de ser salvaguardados"[18].

[17] DOMÍNGUEZ ÁLVAREZ, J.L. (2020), *ob. cit.*, p. 613.
[18] *Ibidem.*

De esta manera, el artículo 9.2.c) RGPD al referirse al *tratamiento necesario* para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento, en referencia al tratamiento de categorías especiales de datos personales, otorgaría la licencia de no aplicar el artículo 9.1 RGPD. Por consiguiente, el artículo 9.1 RGPD establece una prohibición general, que admite excepciones el artículo 9.2. A su vez, hay que tener en cuenta las letras b), g), i) y h) del artículo 9.2.

En todo caso, las excepciones del artículo 9.2 RGPD deben ser aplicadas teniendo en cuenta el artículo 5 RGPD que expone los principios relativos al tratamiento. Entre los principios, debemos tener en cuenta el principio de licitud, lealtad y transparencia, el principio de limitación de la finalidad, el principio de exactitud y, especialmente, el principio de minimización *"*garantizando que los datos tratados serán exclusivamente los necesarios para la finalidad pretendida, sin que se pueda extender dicho tratamiento a cualesquiera otros datos personales no estrictamente necesarios para dicha finalidad, sin que pueda confundirse conveniencia con necesidad, porque el derecho fundamental a la protección de datos sigue aplicándose con normalidad, sin perjuicio de que, como se ha dicho, la propia normativa de protección de datos personales establece que en situaciones de emergencia, para la protección de intereses esenciales de salud pública y/o vitales de las personas físicas"[19].

Buena parte de los datos relativos a la salud van a aparecer en la denominada "historia clínica" del paciente. En este sentido, la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica (en adelante LAP), en su artículo 3, define la historia clínica como *"el conjunto de documentos que contienen los datos, valoraciones e informaciones de cualquier índole sobre la situación y la evolución clínica de un paciente a lo largo del proceso asistencial"*. Más adelante, el artículo 15.2 LAP, afirma que la finalidad de la historia clínica, no es otra que, *"facilitar la asistencia sanitaria, dejando constancia de todos aquellos datos que, bajo criterio médico, permitan ese conocimiento veraz y actualizado del estado de salud del paciente"*.

Como es obvio, la historia clínica conlleva un tratamiento de datos. No obstante, no es necesario que el médico o el centro sanitario solicite el consentimiento a los pacientes para la recogida y utilización de datos personales y de salud si se van a utilizar

[19] DOMÍNGUEZ ÁLVAREZ, J.L. (2020), *ob. cit.*, p. 617.

para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social[20]. Esta posibilidad resulta amparada por el artículo el artículo 6.1.b) RGPD, para las entidades aseguradoras de salud privadas y por el artículo 6.1.c) para la sanidad pública. En el caso del tratamiento de datos por razones de interés público, la legitimación se encuentra en el artículo 6.1e) RGPD. Como ya vimos, también se pueden tratar los datos de salud sin solicitar el consentimiento cuando el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento, o cuando lo solicite un órgano judicial[21], cuya base legitimadora se encuentra en el artículo 6.1.d) RGPD. Así mismo, dado que estos datos son tratados por personas, el artículo 16.6 LAP deja claro que el personal que accede a los datos de la historia clínica en el ejercicio de sus funciones queda sujeto al deber de secreto.

2.4. USO DE LAS TECNOLOGÍAS CONTRA LA COVID-19

2.4.1. Títulos de legitimación

El uso de las tecnologías y los datos digitales se sitúan como protagonistas siendo un instrumento crucial para hacer frente a la crisis sanitaria provocada la Covid-19. Sin embargo, tal y como alerta la Comisión Europea en su Recomendación 2020/518 relativa a un conjunto de instrumentos comunes de la Unión para la utilización de la tecnología y los datos a fin de combatir y superar la crisis de la Covid-19, en particular por lo que respecta a las aplicaciones móviles y a la utilización de datos de movilidad anonimizados, *"un enfoque fragmentado y descoordinado del empleo de nuevas tecnologías basadas en el tratamiento de datos personales pone en peligro la eficacia de las medidas destinadas a combatir la crisis de la COVID-19, dañando gravemente tanto al mercado único como los derechos y libertades fundamentales"*[22]. En la misma línea, la Agencia Española de Protección de datos (en adelante, AEPD) pone de relieve que en el tratamiento de las tecnologías de la información se debe poner en funcionamiento un plan global común,

[20] AEPD (2019): *Guía para pacientes y usuarios,* p. 6.
[21] *Ibidem.*
[22] Recomendación (UE) 2020/518 de la Comisión, de 8 de abril de 2020, relativa a un conjunto de instrumentos comunes de la Unión para la utilización de la tecnología y los datos a fin de combatir y superar la crisis de la COVID-19, en particular por lo que respecta a las aplicaciones móviles y a la utilización de datos de movilidad anonimizados.

consideración avalada por la mencionada Recomendación (UE) 2020/518 de la Comisión de 8 abril 2020[23].

La puesta en marcha de aplicaciones móviles sobre la base del manejo de datos personales hace que éstas proporcionen información sobre todos los aspectos de la crisis sanitaria, permiten mejorar la capacidad de previsión y decisión de las autoridades sanitarias y contribuyen a fortalecer la eficacia de las medidas de distanciamiento social, reduciendo con ello significativamente la propagación de la pandemia[24].

Así las cosas, el RGPD contiene protecciones y reglas necesarias que permiten en diversas situaciones, incluida la situación de emergencia sanitaria. Atendiendo al considerando 46 del RGPD, mencionado anteriormente, la base jurídica en lo referente al tratamiento de datos puede ser múltiple. Centrándonos en el tratamiento de datos de salud, no resulta suficiente la legitimación del artículo 6 RGPD, sino que debemos acudir al artículo 9 RGPD, debido a que los datos de salud son una categoría especial de datos. Como sabemos, el artículo 9.2 RGPD establece varios títulos de legitimación que permite el tratamiento. Entre ellas, cabe destacar para el objeto de nuestro estudio las siguientes:

En la letra b), hace referencia al ámbito laboral en las relaciones entre empleado y empleador, cuando el tratamiento es necesario en atención a las obligaciones del empleador. En este sentido, la Ley 31/1995, de 8 de noviembre de prevención de riesgos laborales, exige que el empresario garantice la protección de los trabajadores frente a los riesgos laborales. En el contexto de la emergencia sanitaria deriva de la Covid-19 el trabajador tiene, por ello, el deber de informar al empresario sobre todo lo relacionado con el virus cuando éste pueda o crea estar afectado, de esa manera se protege su salud y la del resto de los trabajadores de la empresa.

Las letras g) y i) se refieren a la existencia del interés público. La primera contempla un interés público esencial y la segunda pone de manifiesto un interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud. Todo ello sobre la base del Derecho de la Unión o de los Estados

[23] La Recomendación (UE) 2020/518 de la Comisión, de 8 de abril de 2020 establece un proceso destinado a desarrollar un enfoque común, denominado "conjunto de instrumentos", con el fin de usar los medios digitales para hacer frente a la crisis. El conjunto de instrumentos se centra en la atención de dos aspectos: 1) un enfoque paneuropeo para el uso de aplicaciones móviles, coordinado a nivel de la Unión y 2) un plan común para el uso de datos anonimizados y agregados sobre la movilidad de la población.
[24] DOMÍNGUEZ ÁLVAREZ, J.L. (2020), *ob. cit.*, p. 610.

Miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional.

La letra h) se refiere al supuesto de que el tratamiento sea necesario para realizar un diagnóstico médico, o evaluación de la capacidad de laboral del trabajador o cualquier otro tipo de asistencia de tipo sanitario o para la gestión de los sistemas y servicios de asistencia sanitaria y social.

Por último, la letra c) permite el tratamiento cuando es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento[25].

Atendiendo a la legislación nacional, la AEPD, en su informe 17/2020, de 12 de marzo[26], ha señalado expresamente que el tratamiento de datos sin consentimiento podría derivar de lo dispuesto en diferentes normas sanitarias:

a) El artículo 26 de la Ley 14/1986, de 25 de abril, General de Sanidad, por el que se atribuye competencias a los servicios sanitarios ante la existencia de un riesgo inminente y extraordinario para la salud.
b) La Ley Orgánica 3/1986, de 14 de abril, de Medidas Especiales en Materia de Salud Pública (modificada mediante Real Decreto-ley 6/2020, de 10 de marzo, por el que se adoptan determinadas medidas urgentes en el ámbito económico y para la protección de la salud pública) que habilita para el control de los enfermos.
c) La Ley 33/2011, de 4 de octubre, General de Salud Pública que, amén de garantizar el derecho fundamental a la protección de datos en su artículo 9, establece el deber de todas las personas de comunicar datos o circunstancias que pudieran constituir un riesgo o peligro grave para la salud.
d) El párrafo segundo apartado c) de la disposición adicional decimoséptima sobre tratamientos de datos de salud de la LOPDGDD, habilita al uso de datos con fines de investigación en salud pública sin consentimiento en circunstancias como una epidemia."

Por ello el informe de la AEPD concluye que "desde un punto de vista de tratamiento de datos personales, la salvaguardia de intereses esenciales en el ámbito de la

[25] Sobre los títulos de legitimación, *vid*. DOMÍNGUEZ ÁLVAREZ, J.L. (2020), *ob. cit.*, p. 613.
[26] AEPD (2020): Informe AEPD N/REF: 0017/2020, de 12 de marzo, avala todos aquellos tratamientos necesarios para alcanzar los objetivos de salud pública, p.6.

salud pública corresponde a las distintas autoridades sanitarias de las diferentes administraciones públicas, quienes podrán adoptar las medidas necesarias para salvaguardar dichos intereses esenciales públicos en situaciones de emergencia sanitaria de salud pública".

2.4.2. La aplicación *Radar Covid*

Un buen ejemplo de la necesaria compatibilidad entre el progreso tecnológico y protección de datos se traduce en la aparición de aplicaciones móviles de alerta de contagios del virus SARS-CoV-2[27], entre las que se encuentra en la aplicación *Radar Covid*.

La Comisión Europea en su Recomendación (UE) 2020/518 de 8 de abril de 2020[28] ha definido lo que debemos entender por "aplicación móvil": *"las aplicaciones de soporte lógico (software) que se ejecutan en dispositivos inteligentes, en particular teléfonos inteligentes, diseñadas generalmente para una interacción amplia y específica con recursos web, que procesan datos de proximidad y otra información contextual recogida por los distintos sensores presentes en cualquier dispositivo inteligente, y que pueden intercambiar información a través de diversas interfaces de red con otros dispositivos conectados"*.

En este sentido la aplicación *Radar Covid* es una aplicación móvil de alerta de contagios del virus SARS-CoV-2 desarrollada por el Gobierno de España, a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial del Ministerio de Asuntos Económicos y Transformación Digital. La aplicación ayuda a controlar la propagación de la Covid-19 a través de la identificación de los posibles contactos estrechos de casos confirmados a través de la tecnología *Bluetooth*[29].

El *quid* de la aplicación estriba en que el usuario se descarga la aplicación de forma voluntaria, de manera que, una vez que acepta su uso, la aplicación le alerta a través de una notificación en caso de que en un espacio temporal "de catorce días anteriores a esa notificación hayan estado expuestos a un contacto epidemiológico —a menos de dos

[27] DOMÍNGUEZ ÁLVAREZ, J.L. (2020), *ob. cit.*, p. 621.
[28] Recomendación (UE) 2020/518 de la Comisión de 8 de abril de 2020, relativa a un conjunto de instrumentos comunes de la Unión para la utilización de la tecnología y los datos a fin de combatir y superar la crisis de la COVID-19, en particular por lo que respecta a las aplicaciones móviles y a la utilización de datos de movilidad anonimizados.
[29] *Vid.* web sobre *Radar COVID*. Disponible en: https://radarcovid.gob.es/faq-informacion-general

metros y más de 15 minutos— con otro usuario —totalmente anónimo— que haya declarado en la aplicación haber dado un resultado positivo en la prueba de COVID-19, previa acreditación por parte de las autoridades sanitarias correspondientes"[30]. En todo caso, la aplicación sólo informa del día, dentro del periodo de referencia de 14 días, en que se haya producido la exposición al virus, preservando la identidad del usuario al que haya quedado expuesto y protegiendo la identificación del dispositivo de este. Por consiguiente, se ha logrado desarrollar una herramienta digital que permite incrementar "la capacidad de rastreo de propagación del virus de las autoridades sanitarias al tiempo que se establecen elevados estándares de protección de la privacidad, ya que la aplicación no solicita, utiliza ni almacena datos de carácter personal de los usuarios, tal y como se desprende tanto de su política de privacidad como de las afirmaciones de los responsables de dicha herramienta digital"[31].

Respecto al funcionamiento de la aplicación, hay que destacar que una vez que el usuario se haya descargado la aplicación, éste debe aceptar las condiciones de uso y la política de privacidad. Por consiguiente, el dispositivo móvil va a producir cada día un identificador pseudo-aleatorio conocido como "clave de exposición temporal" que servirá para derivar los "identificadores efímeros Bluetooth" que son intercambiados con otros teléfonos móviles próximos que también tengan descargada la aplicación *Radar Covid*[32].

En términos generales, el éxito de las aplicaciones móviles como herramienta de apoyo en pro de la contención de la Covid-19 depende de la colaboración ciudadana en el uso de las mismas. El papel de las autoridades sanitarias es crucial pues una tarea de concienciación, información y garantía del respeto del derecho a la protección de datos

[30] DOMÍNGUEZ ÁLVAREZ, J.L. (2020), *ob. cit.*, p. 618.
[31] *Ibidem*, p. 618.
[32] Ibidem, p. 618. El autor explica que "los 'identificadores efímeros Bluetooth' son una serie de códigos pseudo- aleatorios con un tamaño de 16 caracteres (16 bytes, o 128 bits), que se generan por cada uno de los diferentes dispositivos móviles cada 10-20 minutos, a partir de la "clave de exposición temporal" diaria. Lo más relevante de estos códigos es que los mismos no contienen ningún tipo de información personal, que permita identificar directa o indirectamente al dispositivo o al usuario del mismo, protegiendo con ello los datos relativos a la salud de los pacientes en todo momento al tiempo que se erige como un instrumento respetuoso para con los derechos fundamentales de la ciudadanía, y muy especialmente en lo que atañe a la protección de datos de carácter personal. Por tanto, la aplicación descarga periódicamente las claves de exposición temporal compartidas voluntariamente por los usuarios diagnosticados por COVID-19 del servidor, para compararlas con los códigos aleatorios registrados en los días anteriores como resultado de contactos con otros usuarios. Si se encuentra una coincidencia, la aplicación ejecuta un algoritmo en el dispositivo que, en función de la duración y la distancia estimada del contacto, y de acuerdo con los criterios establecidos por las autoridades sanitarias, decide si se muestra una notificación en el dispositivo del usuario expuesto al riesgo de contagio, advirtiéndole del contacto, comunicándole la fecha del mismo e invitándolo a auto-confinarse, y contactar con las autoridades sanitarias".

puede ser clave para la implementación de las herramientas tecnológicas que tenemos a nuestro alcance[33].

La aplicación ha recibido denuncias presentadas ante la Secretaría General de Administración Digital por omisión del estudio de impacto sobre protección de datos y de otros aspectos preceptivos[34]. No obstante, a tenor de las declaraciones de los responsables de la AEPD, no parece en principio que dichas denuncias vayan a progresar, al manifestarse que *"en el plano teórico, cumple con los criterios del Comité Europeo de Protección de Datos"*, aunque la Agencia mantiene una investigación abierta para analizar en profundidad el tratamiento de datos personales que realiza la app[35].

2.4.3. Geolocalización

El Comité Europeo de Protección de Datos (CEPD), de acuerdo con las Directrices 04/2020, de 21 de febrero, sobre el uso de datos de localización y herramientas de rastreo de contactos en el contexto de la pandemia de COVID-19, proporciona una definición de "*datos de localización*", que comprende:

> "*todos los datos tratados en una red de comunicaciones electrónicas o por un servicio de comunicaciones electrónicas que indican la posición geográfica del equipo terminal de un usuario de un servicio de comunicaciones electrónicas disponible para el público (según la definición de la Directiva*[36]*), así como a los datos de otras posibles fuentes, relativos a: la latitud, longitud o altitud del equipo terminal, la dirección del desplazamiento del usuario, o el momento en el que se registró la información sobre la localización"*[37].

En este sentido, REVENGA SÁNCHEZ ha explicado que las aplicaciones de rastreo de contactos fueron utilizadas por primera vez en Singapur a los pocos días de la declaración de la pandemia (*TraceTogether*). Desde entonces las *apps* de rastreo han sido

[33] En el mismo sentido, DOMÍNGUEZ ÁLVAREZ, J.L. (2020), *ob. cit.*, p. 618.
[34] REVENGA SÁNCHEZ, M. (2020): "La pandemia y el derecho a la intimidad", Revista Catalana de Dret Públic, Extraordinario nº 3, pp. 134, menciona también no haber definido con la suficiente precisión las finalidades del tratamiento, las funciones y las responsabilidades de las autoridades sanitarias de las comunidades autónomas, y los plazos de conservación de los datos.
[35] UIMP (2020): "Mar España Martí, directora de la AEPD: La protección de datos es un derecho fundamental que sigue plenamente vigente durante el COVID-19". Disponible en: http://www.uimp.es/actualidad-uimp/mar-espana-marti-la-proteccion-de-datos-es-un-derecho-fundamental.html
[36] Se refiere a la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas.
[37] Apartado 2 del Anexo (Definiciones).

objeto de permanente debate sobre sus supuestos beneficios y debilidades. Se trata de un beneficio sujeto a condición: para cumplir las expectativas, las apps tendrían que ser descargadas y activadas masivamente. En unos casos se presentan como una panacea, un ejemplo elocuente de lo importante que puede resultar para la salud pública el recurso a las nuevas tecnologías. Por el contrario, otros contemplan las apps de rastreo de contactos como peligrosos artefactos que no harán sino incrementar el control sobre nuestras vidas e infligir otra vuelta de tuerca en la erosión irreversible del derecho a la intimidad[38].

En el uso de los datos de localización e instrumentos de rastreo hay que tener en cuenta los principios y condiciones que matizan y precisan las propias Directrices 04/2020. De manera que se establecen para dos fines concretos, según su parágrafo 5: a) el uso de datos de localización para apoyar la respuesta a la pandemia mediante la modelización de la propagación del virus; y b) el rastreo de contactos, cuyo objetivo es que las personas que hayan estado muy cerca de alguien que resulte ser un portador confirmado del virus sean informadas al respecto, a fin de romper las cadenas de transmisión lo antes posible.

En todo caso, hay que aclarar que el uso de las herramientas de rastreo de contactos es voluntario y arrojan una información de proximidad, de modo que la herramienta no proporciona un rastreo individual.

Respecto de los datos de localización, podemos distinguir dos fuentes principales, de acuerdo con el parágrafo 9. De un lado, los datos de localización recogidos por proveedores de servicios de comunicaciones electrónicas (caso de los operadores de comunicaciones móviles) en el contexto de la prestación de sus servicios. Por otra parte, los datos de localización recogidos por las aplicaciones de los proveedores de servicios de la sociedad de la información cuya funcionalidad requiere el uso de dichos datos (aplicaciones de navegación, servicios de transporte, etc.).

El tratamiento de los datos de localización está sujeto a límites, localizados en los artículos 6 y 9 de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas. En cuanto a la información, incluidos los datos de localización, obtenida directamente de los equipos terminales, es de aplicación el artículo 5.3 de la Directiva 2002/58/CE, de modo que el almacenamiento de información en el dispositivo del usuario o la obtención de acceso a la información ya

[38] REVENGA SÁNCHEZ, M. (2020): "La pandemia y el derecho a la intimidad", *Revista Catalana de Dret Públic*, Extraodinario nº 3, p. 133.

almacenada solo se permite cuando i) el usuario haya dado su consentimiento[39] , o cuando ii) el almacenamiento y/o acceso sea estrictamente necesario para la prestación del servicio de la sociedad de la información expresamente solicitado por el usuario. No obstante, cabe establecer excepciones a los derechos y obligaciones contemplados en la Directiva en virtud de su artículo 15, cuando constituyan una medida necesaria, adecuada y proporcionada en una sociedad democrática para cumplir determinados objetivos"[40].

Cabe preguntarse si es posible la reutilización de los datos de localización. Debe ponerse de relieve que el legislador aboga por una protección adicional dada la sensibilidad de estos datos, pues suponen una injerencia en la persona y hay que recordar que los datos que se ceden son datos de salud y de localización. De manera que cuando los datos hayan sido recogidos sobre la base de la legitimación arrojada por el artículo 5.3 de la Directiva 2002/58/CE, para que quepa la reutilización de estos datos es necesario contar con el consentimiento adicional del usuario o bien apoyarse en una disposición de la Unión o del Estado miembro que constituya una medida necesaria y proporcionada en una sociedad democrática para proteger los objetivos a que se refiere el artículo 23.1 RGPD[41].

Dentro de los datos de localización, el Comité Europeo de Protección de Datos sienta la preeminencia del uso de datos de localización anonimizados. La anonimización se define como el "*uso de un conjunto de técnicas destinadas a suprimir la capacidad de asociar los datos a una persona física identificada o identificable mediante un esfuerzo «razonable»".* El Comité subraya que esta «prueba de razonabilidad» debe tener en cuenta tanto los aspectos objetivos (tiempo, medios técnicos) como los elementos contextuales, que pueden variar de un caso a otro (carácter excepcional de un fenómeno teniendo en cuenta, por ejemplo, la densidad de la población y la naturaleza y volumen de los datos). Si los datos no superan esta prueba, no se han anonimizado y, por tanto, se mantienen dentro del ámbito de aplicación del RGPD. Por último, dada la complejidad de los procesos de anonimización, el CEPD recomienda la transparencia en lo que respecta a la metodología de anonimización"[42].

En lo que se refiere a la legitimidad del uso de la aplicación en sí misma, la legitimación parte de la base, como hemos señalado anteriormente, de su acogimiento

[39] El concepto de consentimiento recogido en la Directiva está sujeto al cumplimiento de todos los requisitos del consentimiento previstos en los artículos 4.11 y 7 RGPD.
[40] Parágrafos 11 y 12 de las Directrices 04/2020.
[41] Parágrafo 13 de las Directrices 04/2020.
[42] Parágrafos 13 a 23 de las Directrices 04/2020.

voluntario por el usuario. A su vez, es fundamental que se garantice la rendición de cuentas, es decir, debe precisarse quiénes son los responsables del tratamiento de datos en esta clase de aplicaciones[43]. Sólo así se garantiza el compromiso del uso de las herramientas tecnológico bajo el paraguas de la legitimidad y la legalidad.

Debemos traer a colación de nuevo los principios relativos al tratamiento de datos del artículo 5 RGPD para ver cómo se insertan y se aplican específicamente con respecto a las aplicaciones de rastreo de contactos, dado que reforzar la transparencia de los perfilados y tratamientos automatizados es clave para la confianza social [44]. Para ello es preciso poner de relieve la importancia del principio de finalidad y el principio de minimización de datos. El primero de ellos -principio de finalidad- es clave en esta materia, pues las finalidades deben ser lo suficientemente específicas para que en el caso de una reutilización de los datos de localización este principio se sitúe como posible hilo conductor hacia un tratamiento ulterior de datos o no. Es decir, si se trata de fines extraños o no a la crisis sanitaria.

Especial hincapié se debe hacer también con respecto al principio de minimización de datos, que en esta materia tienen varios requisitos o recomendaciones del Comité. En primer lugar, las aplicaciones de rastreo de contactos no requieren un seguimiento de la ubicación de los usuarios a título individual; en su lugar, deben utilizarse datos de proximidad; en segundo lugar, como se trata de aplicaciones que pueden funcionar sin la identificación directa de personas, conviene establecer medidas adecuadas para prevenir la reidentificación; por último, la información recogida debe alojarse en el equipo terminal del usuario y solo debe recogerse la información pertinente cuando sea absolutamente necesario. [45]

Por tanto, los datos objeto de tratamiento deben reducirse a los mínimos estrictamente necesarios, de modo que la aplicación no recoja datos que no tengan que ver con el objeto específico de la misma (por ejemplo: el estado civil de la persona).

El CEPD señala que en las aplicaciones de rastreo de contactos la base jurídica sobre la que se ampara el tratamiento de datos debe incorporar salvaguardias significativas.

[43] En opinión del CEPD, podrían serlo las autoridades sanitarias nacionales, aunque cabe prever también otras fórmulas. En todo caso, si el despliegue de aplicaciones de rastreo de contactos implica a diferentes agentes, es importante que sus funciones y responsabilidades estén claramente delimitadas desde el principio y que se expliquen a los usuarios (Parágrafo 25 de las Directrices 04/2020).

[44] COTINO HUESO, L. (2020). "Inteligencia artificial, big data y aplicaciones contra la COVID-19: privacidad y protección de datos". *IDP: Revista de Internet, Derecho y Política*, nº 31, p. 12.

[45] Parágrafo 27 de las Directrices 04/2020.

Por ello, debemos traer a colación el ya mencionado artículo 5.3 de la Directiva 2002/58/CE, si tales operaciones son estrictamente necesarias para que el proveedor de la aplicación preste el servicio solicitado explícitamente por el usuario, el tratamiento no requerirá su consentimiento. En el caso de las operaciones que no sean estrictamente necesarias, el proveedor deberá pedir el consentimiento del usuario.[46]

A su vez, el CEPD establece una matización importante y es que el hecho de que la aplicación móvil solicite al usuario la aceptación de política y condiciones, no significa que la legitimidad del tratamiento de datos esté basada en el consentimiento del mismo. Por consiguiente, la legitimidad tanto del uso como del tratamiento se encuentra en el artículo 6.1.e) RGPD, que lo permite cuando su finalidad obedezca al cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. Ahora bien, si el tratamiento de datos se apoya en el consentimiento del artículo 6.1.a) RGPD el responsable del tratamiento tendrá la obligación de velar por que se cumplan los estrictos requisitos necesarios para dotar de validez a ese fundamento jurídico[47].

No hay que olvidar que el uso de la aplicación implica que la misma va a llevar a cabo una recogida de datos de salud si pensamos, por ejemplo, que un usuario resulta positivo. Conviene recordar a estos efectos las excepciones que ampara el artículo 9.2 RGPD, en especial la letra i) [conforme a la cual, el tratamiento de datos está permitido por razones de interés público en el ámbito de la salud pública]; la letra h) [tratamiento para fines de asistencia sanitaria]; la letra j) [tratamiento para para fines de investigación científica o fines estadísticos]; por último, como se ha señalado antes, dependiendo de la base jurídica, el tratamiento también puede venir legitimado por el consentimiento, letra a)[48].

Finalmente, cabe realizar una consideración final respecto a estas aplicaciones móviles de rastreo, de modo que resulta preciso ser especialmente cuidadoso con el tratamiento de las mismas, dado que presentan simultáneamente importantes beneficios pero también riesgos[49].

[46] Parágrafo 27 de las Directrices 04/2020.
[47] Parágrafos 31-32 de las Directrices 04/2020.
[48] Parágrafos 33 de las Directrices 04/2020.
[49] Como señala REVENGA SÁNCHEZ, incorporar a nuestros teléfonos una aplicación que nos pone en contacto permanente con los otros y permite a las autoridades sanitarias alertarnos de situaciones de riesgo según lo que resulte de tal contacto no es cosa baladí. Por lo pronto, nos viene a mostrar que la telemedicina está ya aquí, y, como suele decirse con la recurrente frase hecha, ha venido para quedarse. Por ahora se trata

2.4.4. Toma de temperatura

Tras el confinamiento una de las medidas que se ha adoptado con el objetivo de prevenir contagios por Covid-19 ha sido la toma de temperatura corporal. Esta medida se ha establecido de forma generalizada con el objetivo de determinar si una persona en base a su temperatura puede acceder o no a centros de trabajo, comercios, centros educativos u otro tipo de establecimientos.

La AEPD, en su Comunicado de 30 de abril de 2020, ha mostrado su preocupación por esta medida, pues se está llevando a cabo sin la previa y necesaria decisión de las autoridades sanitarias. En este sentido, la toma de temperatura es un dato personal y no debe considerarse como un hecho aislado en sí mismo. Por tanto, como dato personal de salud, implica un tratamiento que debe adecuarse a la legislación correspondiente. En particular, la aplicación de esta medida requiere la determinación previa que haga la autoridad sanitaria competente.

El talón de Aquiles de la medida radica en que la temperatura no es un indicio suficiente de la enfermedad, ya que existe un alta porcentaje de personas contagiadas que son asintomáticas y no presentan fiebre. Las autoridades sanitarias también han podido saber a través de estudios realizados, que personas que sí son sintomáticas y tampoco presentan fiebre, en particular en las primeras fases de la enfermedad. A su vez, la temperatura corporal no es la misma en todos los seres humanos, por lo que es absolutamente necesario seguir los criterios de las autoridades sanitarias para obtener resultados homogéneos basados en evidencias científicas en orden a mismos criterios y no resultados heterogéneos con criterios dispares. Ante esta realidad, la AEPD apuesta por otras medidas menos intrusivas y que tengan la misma eficacia[50]

En lo referente al tratamiento de datos, al igual que el resto de datos relativos a la salud, debe regirse por los mencionados principios del RGPD y entre ellos, el principio de legalidad. La base legitimadora para el tratamiento de datos de temperatura, como categoría especial de datos se encuentra en los artículos 6.1 y 9.2 RGPD.

---

de una telemedicina que es solo muy genérica y de carácter preventivo, pero, nos guste o no, a través de las apps de rastreo se acaba realizando un prediagnóstico sobre nuestra exposición al virus basado en el control permanente de nuestra conducta (REVENGA SÁNCHEZ, M. (2020), ob. cit., p. 133).

[50] Comunicado de la AEPD en relación con la toma de temperatura por parte de comercios, centros de trabajo y otros establecimientos de 30 de abril de 2020. Disponible en:
https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/comunicado-aepd-temperatura-establecimientos

Respecto a la toma de temperatura en el ámbito laboral, ya hemos hecho referencia en este trabajo a que, tratándose de un dato de salud, la base jurídica para el tratamiento de estos datos deriva del deber que tiene el empleador de garantizar la seguridad y salud de los trabajadores a su servicio en los aspectos relacionados con el trabajo. Dentro del ámbito laboral, la AEPD afirma que, considerando la base jurídica mencionada desde un punto de vista amplio, "podría extenderse a un centro o local que estén destinados a unas finalidades específicas y que en ellos se concentren un elevado número de clientes o usuarios ajenos a la empresa que los gestiona, siempre estarán presentes en ellos personas trabajadoras sobre las que el empleador mantiene sus obligaciones. Esta aproximación requiere de una adecuada ponderación entre el impacto sobre los derechos de los clientes o usuarios de estas medidas y el impacto en el nivel de protección de las personas empleadas. Esa ponderación debe obedecer a criterios establecidos por las autoridades sanitarias".[51]

Acudiendo otra base jurídica diferente, la del artículo 9.2 i) RGPD -tratamiento de datos por razones de interés público en el ámbito de salud pública-, según el comunicado de la AEPD requeriría "un soporte normativo a través de leyes que establezcan ese interés y que aporten las garantías adecuadas y específicas para proteger los derechos y libertades del interesado." La AEPD, realiza una matización al respecto y es que la utilización del interés legítimo de los responsables del tratamiento como base legitimadora quedaría en todo caso excluida por un doble motivo. En primer lugar, ninguna disposición del artículo 9.2 RGPD permite el levantamiento de la prohibición de tratamiento de datos sensibles por razones de interés legítimo (salvo que en determinadas materias así lo contemple el derecho de la Unión o de los Estados Miembros). En segundo lugar "porque el impacto de este tipo de tratamientos sobre los derechos, libertades e intereses de los afectados haría que ese interés legítimo no resultara prevalente con carácter general"[52].

En relación con los datos de temperatura hay que traer a colación el principio de limitación de la finalidad del artículo 5 RGPD. Este principio, según la AEPD, supone "que los datos de temperatura solo pueden obtenerse con la finalidad específica de detectar posibles personas contagiadas y evitar su acceso a un determinado lugar y su contacto dentro de él con otras personas." De esta manera, esos datos no pueden ser utilizados para otra finalidad. Añade que "este principio resulta especialmente aplicable en el supuesto de que los datos de temperaturas se obtengan utilizando dispositivos como, por ejemplo, el

[51] *Ibidem.*
[52] *Ibidem.*

caso de las cámaras térmicas que ofrecen la posibilidad de grabar y conservar los datos o tratar información adicional, en particular, información biométrica"[53].

También entra en juego también el principio de exactitud que supone "que los equipos de medición que se empleen deben ser los adecuados para poder registrar con fiabilidad los intervalos de temperatura que se consideren relevantes." La garantía de que los equipos de medición son válidos es a través de la utilización de equipos homologados.

Por tanto, la toma de temperatura supone un tratamiento de categorías especiales de datos que debe respetar los ya mencionados principios de legalidad, finalidad y exactitud.

En último lugar, es importante ponernos en la posición de los afectados por estas medidas para ver los derechos y las garantías de los mismos. En el caso de tratamiento de este tipo de datos, "los afectados siguen manteniendo sus derechos y garantías de acuerdo con el RGPD si bien adaptadas a las condiciones y circunstancias específicas de este tipo de tratamiento". Por consiguiente, "hay que tener en cuenta las medidas relativas a la información a los trabajadores, clientes o usuarios sobre estos tratamientos (en especial si se va a producir una grabación y conservación de la información) u otras para permitir que las personas en que se detecte una temperatura superior a la normal puedan reaccionar ante la decisión de impedirles el acceso a un recinto determinado (por ejemplo, justificando que su temperatura elevada obedece a otras razones). Para ello, el personal deberá estar cualificado para poder valorar esas razones adicionales o debe establecerse un procedimiento para que la reclamación pueda dirigirse a una persona que pueda atenderla y, en su caso, permitir el acceso."

Con respecto a los plazos y criterios de conservación, en el caso de que sean registrados, "en principio, y dadas las finalidades del tratamiento, este registro y conservación no debieran producirse, salvo que pueda justificarse suficientemente ante la necesidad de hacer frente a eventuales acciones legales derivadas de la decisión de denegación de accesos". Por último, la AEPD señala que la comunicación se refiere con carácter general a cualquier proceso de toma de temperatura en los escenarios más probables".[54]

Resta efectuar una referencia final a las denominadas *cámaras térmicas.* Se trata de un tipo de cámaras que añaden la capacidad de tomar la temperatura a los individuos que

[53] *Ibidem.*
[54] *Ibidem.*

cruzan un área, sin requerir en muchos casos ninguna acción por su parte. Dichas cámaras identifican mediante algoritmos de inteligencia artificial los rostros humanos, los discriminan del resto de elementos que aparecen en la imagen y revelan la temperatura corporal aproximada de cada individuo. La AEPD también ha manifestado su preocupación sobre el uso de estos dispositivos y la necesidad de contar con el criterio previo de las autoridades sanitarias antes de proceder a su instalación[55].

3. EL MODELO LAXO DE PROTECCIÓN DE DATOS EN EMIRATOS ÁRABES UNIDOS

3.1. INTRODUCCIÓN

Emiratos Árabes Unidos (EAU), como su propio nombre indica, es un país formado por siete emiratos. Cada emirato tiene sus propias leyes y regulaciones, si bien EAU tiene una organización legislativa federal, aplicándose sus leyes a todos los emiratos con ciertas excepciones[56].

Durante los 10 últimos años, EAU ha avanzado considerablemente en materia de privacidad y protección de datos, tanto de personas físicas como de empresas. Debe tenerse en cuenta que se trata de un país muy joven, creado en 1971. Anteriormente, el territorio fue una colonia dependiente de Gran Bretaña. Durante la colonización, las leyes que imperaban en el país eran una copia adaptada y abreviada de las que regían el Reino Unido. Durante la ocupación británica, no hay referencias en sus leyes a la protección de datos o similar[57], y ha sido, desde la independencia de este país cuando se han ido aprobando de forma paulatina[58].

EAU, aunque poseedor de gran riqueza, no experimentó grandes cambios o avances dentro de su territorio durante el último cuarto de siglo. Por el contrario, desde el comienzo del siglo XXI, ha experimentado un crecimiento exponencial tanto a nivel económico, social y por supuesto legislativo. Parte de este crecimiento se debe a la globalización y a la

[55] AEPD (2020): *El uso de las tecnologías en la lucha contra el Covid19. Un análisis de costes y beneficios*, pp.11-12. Disponible en: https://www.aepd.es/sites/default/files/2020-05/analisis-tecnologias-COVID19.pdf
[56] ULRICHSEN, K.C. (2017): *The United Arab Emirates: Power, Politics and Policy Making*, Routledge, Nueva York.
[57] Cfr. HEARD-BEY F. (2017). *Abu Dhabi, the United Arab Emirates and the Gulf Region: Fifty Years of Transformation*, Gerlach Press, Berlin.
[58] ULRICHSEN, K.C. (2017), *ob. cit.*

importación de talentos y empresas al país, que le ha permitido ser competitivo y convertirse en una potencia económica clave a nivel internacional[59]. Todo ello ha contribuido también al desarrollo de una política de privacidad de datos a aplicar en los diferentes ámbitos del territorio.

3.2. NORMATIVA GENERAL EN MATERIA DE PROTECCIÓN DE DATOS

Como el resto de países del Golfo Arábigo, EAU se vale de sus propias leyes nacionales en materia de protección de datos, sin que exista una estructura legislativa transnacional como ocurre en el territorio europeo.

La ley federal nº 5 de 2012, sobre la lucha contra los delitos cibernéticos[60] y su enmienda vía la ley federal nº 12 de 2016[61] son los principales mecanismos normativos en lo que a la protección de datos se refiere. Esta ley sustituye a la ley anteriormente vigente de 2006[62], considerada insuficiente e ineficaz por parte del parlamento y los diferentes actores implicados. La necesidad de adaptación de esta ley vino, por otra parte, condicionada por el *boom* tecnológico de las redes de telefonía, dispositivos móviles y ordenadores con acceso a internet y el auge de las redes sociales que interconectan la información y los informantes globalmente.

Esta normativa de protección de datos prohíbe la ilegalidad de la divulgación o revelación de información obtenida por medios electrónicos, si dicha información ha sido obtenida de manera ilegal o no autorizada. La aplicación se hace efectiva a todos los ámbitos, incluido el sanitario, siendo de obligado cumplimiento por todos los sectores, incluido el gubernamental. Además, la ley requiere que toda entidad que opere dentro del territorio emiratí debe cumplir las reglas de protección de datos establecidas independientemente de cuál sea el domicilio fiscal de la entidad y de si los datos han sido obtenidos dentro del territorio o si esos datos conciernen a habitantes del mismo. En concreto, su artículo 21 establece que la obtención de cualquier tipo de información con propósito de ofender a otro individuo, atacar o invadir su privacidad, puede tener consecuencias penales.

[59] ULRICHSEN, K.C. (2017), *ob. cit.*
[60] Federal Decree-Law no. (5) of 2012, 13 August, on combating cybercrimes. Gaceta oficial del estado número 540.
[61] Federal Law no. (12) of 2016, 25 September, on Regulating the Security Industry in the Emirate of Dubai and its amendments. Official Gazette of the United Arab Emirates, no. 622.
[62] Federal Law no. (2) 2006, 30 January, on the Prevention of Information Technology Crimes. Official Gazette of the United Arab Emirates, no. 540.

A su vez, el artículo 22 de la ley establece que el uso de cualquier dispositivo electrónico, aplicación móvil, sitios web u otros sistemas tecnológicos con el objetivo de obtener información no autorizada o con el propósito de divulgar cualquier información, puede tener implicaciones legales independientemente de que dicha información haya sido demandada por parte del empleador u obtenida a título personal.

El organismo regulador del cumplimiento de las normas de protección de datos en EAU a todos sus niveles es el "*Telecomunications Regulatory Authority*" (Autoridad Reguladora de telecomunicaciones)[63]. Dicha estructura se sirve del *National Media Council* (Consejo Nacional de Medios de Comunicación) y de los dos operadores de telecomunicación oficiales del país (*Du* y *Etisalat*) además de la unidad tecnológica de la policía para el cumplimiento de sus funciones.

Las consecuencias penales derivadas del no cumplimiento de la ley de protección de datos en EAU están recogidas en el artículo 378 del Código Penal[64]. Por otro lado, el artículo 31 de la Constitución de EAU[65] establece que toda persona tiene derecho a comunicar o acceder a información, si dicho acto garantiza su confidencialidad de acuerdo con lo que establece la ley.

3.3. PROTECCIÓN ESPECÍFICA DE DATOS SANITARIOS

Hasta el año 2018, toda la información obtenida en el sector sanitario era exclusivamente regulada mediante la ley federal nº 5 de 2012 sobre la lucha contra los delitos cibernéticos y su enmienda vía la ley federal nº 12 de 2016.

En febrero de 2019, el presidente de EAU promulgó la Ley federal nº 2 de 2019, sobre uso de las Tecnologías de la Información y Comunicación en el ámbito sanitario[66]. Esta ley, complementaria a las citadas anteriormente, por vez primera introduce el concepto de la protección de datos relacionados con el historial médico de un paciente, aplicándose a todas las entidades que operan en EAU, pero también se aplica a todos los seguros de salud que actúen en el extranjero con pacientes residentes en Emiratos (seguros

[63] Federal Law no. (3) 2003, de 15 November, regarding the Organization of Telecommunications Sector and its derivates. Official Gazette of the United Arab Emirates, no. 402.
[64] Código Penal de Emiratos Árabes Unidos, de 8 de diciembre de 1987.
[65] Constitución de Emiratos Árabes Unidos, de 2 de diciembre de 1971, enmendada el 2 de iciembre de 1996.
[66] Federal Law no. (2) 2019, 6 January, on the use of the Information and Communication Technology (ICT) in health fields. Official Gazette of the United Arab Emirates, no. 647.

internacionales). De acuerdo con esta norma, los datos obtenidos de un paciente solo pueden ser utilizados con el propósito de proveer servicios sanitarios adecuados al paciente. En caso contrario, los datos clínicos solo podrían ser utilizados previo consentimiento escrito del paciente.

Uno de los aspectos más impactantes de la nueva ley es que, en un intento de asegurar la máxima confidencialidad, su artículo 13 prohíbe que la información sanitaria obtenida en EAU pueda ser exportada fuera del país a no ser que sea autorizado por la autoridad competente. Además, de acuerdo con el artículo 20, los datos sanitarios obtenidos deben ser conservados durante al menos 25 años desde la obtención de los mismos. Finalmente, ley concluye que todos los datos obtenidos por las diferentes aseguradoras y centros sanitarios, deben ser almacenados y centralizados en un sistema dependiente del Ministerio de Salud y Prevención.

No obstante, existen excepciones. El artículo 16 de la ley ampara la publicación de los datos de un paciente sin su consentimiento para: a) permitir a las aseguradoras y otras entidades verificar el historial sanitario de un paciente para poder calcular el valor de un seguro para ese paciente; b) poder realizar proyectos de investigación aprobados por el gobierno, asegurando que la identidad de los pacientes permanezca anónima.

El incumplimiento de esta ley puede derivar en la pérdida de la licencia para ejercer el negocio en EAU e incluso multas que pueden llegar a un máximo de un millón de *dirhams* (equivalentes a 250.000 euros).

3.4. MEDIDAS DE PREVENCIÓN DEL COVID-19

Al igual que muchos otros países, EAU se ha visto afectada por la crisis del Covid-19. El país ya tuvo contacto con una enfermedad similar denominada MERS (*Middle East Respiratory Syndrome*) ocho años antes, si bien las consecuencias fueron mucho menores sin llegar a producir una epidemia.

EAU, al igual que la mayoría de países, tuvo constancia de Covid-19 en su territorio al principio del año 2020. El primer caso diagnosticado a principios de febrero de 2020 fue el de una mujer de nacionalidad china de 73 años que se recuperó poco después. Las dos primeras muertes a causa de la enfermedad, fueron confirmadas el 20 de marzo del

mismo año[67]. Siguiendo las recomendaciones de la Organización Mundial de la Salud, el país inició una campaña de esterilización de las calles seguido de un confinamiento obligatorio que comenzó a finales de marzo de 2020 y que tuvo una duración de 6 semanas. Una vez este confinamiento hubo terminado, se produjo la apertura progresiva de los diferentes sectores y las fronteras terrestres y aéreas, pero con ciertas restricciones y obligaciones como el uso obligatorio de la máscara sanitaria, el uso de gel hidroalcohólico en diferentes establecimientos, la distancia social obligatoria de dos metros y la prohibición de reunión de más de 6 personas en un mismo hogar o espacio público[68].

3.5. USO DE LAS APLICACIONES DIGITALES MOVILES DURANTE LA PANDEMIA

Al igual que otros países, el gobierno de EAU se ha servido de la tecnología para la gestión y control de la expansión de la enfermedad. Hasta el momento, EAU ha utilizado tres aplicaciones móviles para el seguimiento o *tracing* de la Covid-19. Dichas aplicaciones fueron aprobadas a nivel federal, afectando éstas a todos los emiratos que componen el país. Las dos primeras aplicaciones fueron *Stay Home* y *Trace-Covid*. Las dos tenían carácter voluntario, pero eran obligatorias si el individuo pretendía realizar labores fuera del hogar. Estas aplicaciones realizaban un seguimiento de los movimientos de las personas, pero no las relacionaba directamente con su *status* sanitario. En caso de que una persona diese un resultado positivo, tenía prohibición absoluta de movimiento alguno que no fuese al hospital. A su vez, los contactos directos con estos individuos eran igualmente confinados.

Estas dos aplicaciones fueron remplazadas por una más centralizada denominada *ALHOSN*[69]. Dicha aplicación está unida al carnet de identidad de los Emiratos (*Emirates ID)*, aportando así automáticamente toda la información electrónica de este (dirección, estatus marital, lugar de residencia, trabajo, edad, sexo, religión, datos del seguro médico, historial médico electrónico, viajes al extranjero…). Esta aplicación centraliza a su vez todos los test PCR realizados al usuario en estructuras sanitarias públicas dependientes del

[67] Emiratos Árabes Unidos. Ministerio de Salud y Prevención. 2020. [Consultado el 2 de noviembre de 2020] Disponible en: https://www.mohap.gov.ae/en/AwarenessCenter/Pages/COVID19-Information-Center.aspx
[68] Resolution no. (24) of 2018, 18 April, on publishing health information about communicable diseases.
[69] Decision no. (37) 37 of 2020 on measures violations and fines to curb the spread of the novel coronavirus.

ministerio de sanidad o privadas sin necesidad de haber firmado documento alguno que permitiese a la entidad privada la divulgación de los datos a el ministerio de sanidad[70].

ALHOSN fue diseñada para ejercer un control férreo sobre los diferentes focos de contagio por Covid-19 y para asegurar la no expansión de la enfermedad en el territorio emiratí. Sin esta aplicación, el residente en EAU no puede acceder a otros emiratos que no sea el suyo, ni participar de ciertas actividades grupales (conferencias con presencia física, ciertas actividades lúdicas, procedimientos sanitarios rutinarios…). Además, los viajes al extranjero, tanto de salida como de entrada del país, no están permitidos en caso de no uso de la aplicación.

Según la descripción de *ALHOSN* en su portal web[71], la aplicación rastrea personas que hayan tenido contacto con positivos al Covid-19, usando GPS y tecnología *bluetooth*. Por tanto, el uso de la aplicación obliga a la activación de la localización y el *bluetooth* para su funcionamiento. Según el mismo sitio web, ambos teléfonos intercambian anónimamente la información que se almacena en formato encriptado en la aplicación[72]. De esta manera, las autoridades son capaces de rastrear y contactar aquellas personas que han sido expuestas al riesgo y ser testadas de nuevo. En dicho caso, estas personas deberían realizar una cuarentena y dar dos negativos consecutivos en la prueba PCR. Durante el confinamiento obligatorio, la persona infectada o sospechosa de infección tiene la obligación de mantener activa la aplicación para que se pueda controlar el cumplimiento de la cuarentena tanto en tiempo como en no desplazamiento.

La aplicación, a su vez, divide a las personas en cuatro grupos por colores que son verificados en caso de que la persona quiera realizar una de las actividades antes mencionadas: a) gris (la persona no ha sido todavía testada); verde (la persona ha sido testada y el resultado es negativo. Dicho resultado garantiza el acceso a la mayoría de sitios públicos); rojo (el test más reciente muestra que la persona ha sido testada y el resultado es positivo); y ámbar (la persona necesita ser testada puesto que la aplicación ha detectado que ha habido una posible exposición al Covid-19).

[70] Al Hosn App. Abu Dhabi. National Emergency Crisis and Disasters Management Authority. Ministry of Health.
[71] Ministerio de Salud y Prevención. 2020. [Consultado el 4 de noviembre de 2020]. Disponible en: https://www.alhosnapp.ae/en/home
[72] Al Hosn App. Abu Dhabi. National Emergency Crisis and Disasters Management Authority. Ministry of Health.

En los dos últimos supuestos (rojo y ámbar) un sanitario contacta con el individuo para llevar a cabo las acciones pertinentes; confinamiento y test respectivamente.

Hasta la fecha (marzo de 2021), *ALHOSN* tiene carácter totalmente voluntario salvo para los supuestos descritos anteriormente y para todos aquellos que se hayan sometido a la prueba del Covid-19. De hecho, uno de los requisitos para poder acceder a los resultados de la prueba, es que el individuo descargue la aplicación puesto que es el único modo en el que el paciente tiene acceso a ellos. Como la aplicación está unida al *Emirates ID*, o documento identificativo oficial del país, en caso de que algún organismo necesitase conocer la situación del cliente/paciente, dicha persona solo tendría que presentar su *Emirates ID* y no el teléfono.

Además, el gobierno de EAU, apeló a la "responsabilidad de sus ciudadanos" en cuanto a la ayuda de la gestión de la enfermad. Esto implica que tanto personas infectadas como sanas -no consideradas enfermas a falta de un test que lo confirme- deben reportar su posible contagio por contacto, independientemente de haberse sometido o no a la prueba del Covid-19 en el caso de las sanas. En dicho caso, estas personas estarían obligadas a descargar la aplicación y someterse a un test o confinamiento según sean las indicaciones de las autoridades sanitarias. Además, estas personas tienen obligación de reportar aquellos contactos que han tenido anteriormente con otros individuos, durante cuánto tiempo y en qué lugar.

El incumplimiento de todo lo descrito anteriormente relativo al uso de la aplicación conlleva la sanción de 10.000 *dirhams* (2.500 euros), así como una posible sanción penal si además hay un incumplimiento de la cuarentena pudiendo avocar en la deportación del individuo[73].

3.6. *ALHOSN* Y NORMATIVA DE PROTECCIÓN DE DATOS

En teoría, el uso de *ALHOSN* es voluntario, pero en la práctica se convierte en obligatorio en caso de que el individuo tenga intención de participar en algún grado de la vida pública y social del país. Al descargar la aplicación no hay firma de ningún acuerdo o declaración alguna de privacidad. Por el contrario, cuando la aplicación pide acceso al *bluetooth*, localización y la desactivación del ahorro de batería del teléfono (para evitar la inactivación del GPS y bluetooth), el usuario es consciente de que puede ser rastreado o

[73]Federal law no. (2) of 2011, 10 January, In Respect of the Establishment of the National Emergency, Crisis and Disasters Management Authority (NCEMA). Official Gazette of the United Arab Emirates, no. 351.

localizado en alguna medida, puesto que tiene que aceptar esas condiciones para continuar. Una vez superado este paso, la aplicación conecta el número de *Emirates ID* a la base de datos cuando este es introducido manualmente junto con el teléfono.

En teoría la aplicación solamente conecta el *status* sanitario de la persona con la localización GPS y bluetooth en caso de ser positivo a la enfermedad o en caso de haber entrado en contacto con posibles infectados, todo ello con el fin de poder limitar la expansión de la enfermedad y proceder a un test y posible confinamiento. Por tanto, durante este proceso se puede entender que no hay un consentimiento expreso por parte del usuario que descarga la aplicación. Por otro lado, la descarga de la aplicación implica que la persona conoce que la información recabada puede ser utilizada por las autoridades.

En teoría, la información que se intercambia entre los teléfonos es siempre encriptada por medio del STI (*Secure Tracing Identifier*). El gobierno solo accedería al STI de un individuo en caso de que este diese positivo o hubiese sido identificado como agente de riesgo. El acceso al STI no solamente proporciona información relativa al individuo sino también a todos los contactos y movimientos que este ha tenido durante el periodo de tiempo que la aplicación ha estado activa.

Cuando el gobierno lanzó *ALHOSN*, no proporcionó detalles de cómo serían utilizados los datos ni quién tendría acceso a los mismos, además de las propias autoridades sanitarias. El Departamento de Seguridad de Abu Dhabi solamente expresó que la privacidad e información personal de los usuarios sería protegida. Además, no se indicó que se haría con los datos recabados una vez la información no fuese necesaria al fin de la pandemia.

En cuanto a la duración del almacenamiento de los datos, las autoridades publicaron una breve nota explicando que el almacenamiento del STI en la aplicación solo se guardaría durante tres semanas en el teléfono, pero nada se sabe de la información que se actualiza en el servidor donde son recogidos todos los datos. Además, como se mencionó anteriormente, la Ley nº 2 de 2019, sobre uso de las Tecnologías de la Información y Comunicación en el ámbito sanitario, establece que los datos de origen sanitario deben ser almacenados durante 25 años como mínimo.

Finalmente, en un breve apartado de la página web[74] del Ministerio de Sanidad aclaró que la información obtenida vía *ALHOSN*, sólo será utilizada para obtener los resultados de la prueba del Covid-19, pero que no almacenan ni obtienen ninguna información correspondiente a la localización u otro tipo de información personal. Dicha información contrasta con lo especificado en la página web destinada a la introducción y utilidad de *ALHOSN* como ha sido descrito previamente.

4. CONCLUSIONES

La protección de datos ha sido y es un tema de necesario interés por parte de gobiernos, empresas y usuarios o particulares, ya que vivimos en un contexto donde el desarrollo tecnológico se encuentra en continuo crecimiento. Durante la segunda mitad del siglo XX y el siglo XXI la protección de datos ha ido evolucionando y adaptándose para suplir las necesidades derivadas de las nuevas tecnologías. Los diferentes contextos sociopolíticos han hecho que ciertos países cuenten con normativas exigentes de protección de datos comunes, como es el caso de España, en tanto que Estado miembro de la Unión Europea. En cambio, otros países distanciados cultural y geopolíticamente como EUA, cuentan con un régimen de protección de datos menos garantista diferente, fruto de una cultura jurídica diferente.

La protección de datos en España se caracteriza su naturaleza garantista. Ello se traduce en que los datos personales no son de libre acceso en cuanto a su tratamiento. En cambio, EAU, un régimen totalitario, posee un sistema de protección de datos más flexible: aunque, en teoría, los datos personales deben ser protegidos conforme a lo establecido por la ley, *de facto* existe una clara primacía de otros intereses.

La normación de la protección de datos en España y, por ende, de la Unión Europea responde a una configuración del derecho a la protección de datos con carácter no absoluto, lo que implica que debe ejercitarse de acuerdo con el principio de proporcionalidad. Sin embargo, en EAU, no existe tal ponderación de intereses entre el Estado y los titulares del derecho a la protección de datos, produciéndose injerencias de gran calado a la hora de ejercitarlo.

[74] Emiratos Arabes Unidos. Ministerio de Sanidad y Prevención. [Consultado el 7 de noviembre de 2020]. Disponible en: https://www.doh.gov.ae/privacy-policy-alhosn

La situación pandémica producida a nivel global nos lleva a comparar cómo se tratan los datos relativos a la salud en ambos países. En España, los datos de salud gozan de un tratamiento especial, siendo calificados como categoría especial. Ello determina una prohibición general a su tratamiento y unas excepciones, dentro de las cuales se encuentran situaciones de emergencia sanitaria en las que se permite el tal tratamiento, pero estableciendo, en todo caso, garantías para el titular del derecho a la protección de datos. Por consiguiente, el hecho de tratarse de una categoría especial de datos no es óbice para enfrentar la crisis sanitaria a través de instrumentos tecnológicos, siempre bajo determinadas garantías. También en EAU se ha hecho uso de herramientas tecnológicas que implican también el uso de datos relativos a la salud. Sin embargo, no existe una protección garantista sobre los mismos, pese a que se establezcan disposiciones normativas que aparentemente se construyan en aras de proteger el derecho a la confidencialidad.

El Gobierno de EAU pretende una obtención masiva de datos hasta el punto que obliga a las empresas del ámbito sanitario a proporcionar datos de sus usuarios. Un ejemplo de ello, es que, si un paciente se realiza un test PCR en una empresa privada, el gobierno recibirá los resultados de esa prueba de forma simultánea al paciente, siendo visible ese resultado en la aplicación *ALHOSN*, aun no habiendo dado el paciente consentimiento a la empresa privada para que de sus datos y siendo la citada aplicación obligatoria. Por el contrario, en España el uso de la aplicación *Radar Covid* es voluntario y lleva a una recogida de datos de sanitarios. Su tratamiento está permitido por razones de interés público en el ámbito de la salud pública pero está sujeto a limitaciones y garantías en pro de la salvaguarda del derecho a la protección de datos.

La legislación de protección de datos de EAU permite a su vez que las empresas de seguros sanitarios puedan tener acceso a los datos sanitarios de las personas bajo el pretexto de proporcionar servicios sanitarios adecuados al paciente. Ello permite la utilización de datos con fines privados y lucrativos en beneficio de la compañía aseguradora en detrimento de la persona titular de esos datos. En España tal práctica no es admisible al atentar contra los principios de tratamiento de datos establecidos en el RGPD.

Aunque en EUA existan leyes que regulen la protección de datos, en la práctica no existe una tutela eficiente debido a que se trata de normas ambiguas y, en muchos casos, escasamente efectivas. Ello contrasta con la disciplina española en la materia que responde a un modelo garantista.

5. BIBLIOGRAFÍA CITADA

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (2019): *Guía para pacientes y usuarios*. Disponible en:

https://www.aepd.es/sites/default/files/2019-12/guia-pacientes-usuarios-sanidad.pdf

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (2020). Informe Jurídico 0017/2020. Disponible en:

https://www.aepd.es/es/documento/2020-0017.pdf

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (2020). Comunicado de la AEPD en relación con la toma de temperatura por parte de comercios, centros de trabajo y otros establecimientos de 30 de abril de 2020. Disponible en:

https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/comunicado-aepd-temperatura-establecimientos

AEPD (2020): *El uso de las tecnologías en la lucha contra el Covid19. Un análisis de costes y beneficios*. Disponible en

https://www.aepd.es/sites/default/files/2020-05/analisis-tecnologias-COVID19.pdf

CAYÓN DE LAS CUEVAS, J., OCHAGAVÍAS COLAS J.I. (2020): "Overview of the COVID-19 legal framework in Spain: from the state of alarm to the new normal" *EAHL Newsletter*, nº 3, pp. 73-76.

COMITÉ EUROPEO DE PROTECCIÓN DE DATOS (2020): Directrices 04/2020, 21 de abril de 2020, sobre el uso de datos de localización y herramientas de rastreo de contactos en el contexto de la pandemia de COVID-19.

COTINO HUESO, L. (2020). "Inteligencia artificial, big data y aplicaciones contra la COVID-19: privacidad y protección de datos". *IDP: Revista de Internet, Derecho y Política,* nº 31, pp. 1-17.

DOMÍNGUEZ ÁLVAREZ, J.L. (2020). "La necesaria protección de las categorías especiales de datos personales. Una reflexión sobre los datos relativos a la salud como axioma imprescindible para alcanzar el anhelado desarrollo tecnológico frente al COVID-19". *Revista de Comunicación y Salud*, nº 10(2), pp. 607-624.

HEARD-BEY F. (2017). *Abu Dhabi, the United Arab Emirates and the Gulf Region: Fifty Years of Transformation*, Gerlach Press, Berlin

HISCOTT, J., ALEXANDRIDI, M., MUSCOLINI, M., TASSONE. E., PALERMO, E., SOULTSIOTI, M., ZEVINI, A. (2020): "The global impact of the coronavirus pandemic", *Cytokine Growth Factor Rev*, nº 53, pp. 1-9.

KHAN, M., ADIL, S.F., ALKHATHLAN, H.Z., TAHIR, M.N., SAIF, S., KHAN, M., KHAN, S.T. (2021): "COVID-19: A Global Challenge with Old History, Epidemiology and Progress So Far". *Molecules*, nº 26(1), pp. 1-25.

MARTÍNEZ MARTÍNEZ, R. (2020). "Los tratamientos de datos personales en la crisis del COVID-19. Un enfoque desde la salud pública". *Diario La Ley*, nº 9604.

NICOLA, M., ALSAFI, Z., SOHRABI, C., KERWAN, A., AL-JABIR, A., IOSIFIDIS, C., AGHA, M., AGHA, R. (2020): "The socio-economic implications of the coronavirus pandemic (COVID-19): A review". *International Journal of Surgery*, nº 78, pp.185-193.

RALLO LOMBARTE, A. (2019). "El nuevo derecho de protección de datos". *Revista Española de Derecho Constitucional*, 116, pp. 45-74.

REVENGA SÁNCHEZ, M. (2020): "La pandemia y el derecho a la intimidad", *Revista Catalana de Dret Públic*, Extraodinario nº 3, pp. 125-136.

ULRICHSEN, K.C. (2017): *The United Arab Emirates: Power, Politics and Policy Making*, Routledge, Nueva York.